Appendix G

Distributed Computing Environment Test Report

Topic:	Distributed Computing
Subtopic:	Authentication Server Policies and Procedures
Test Objective 244	Verify that Ticket Granting Tickets (TGTs) and service tickets are configured with expiration times, maximum renewal times, and maximum lifetimes.
DII COE SRS Requirement:	None Identified
Rationale:	It is important that these system parameters be configured. They implement a portion of the security policy established by the site.

#	Required Action	Expected Results	Comments	Ö
1	Login to DCE as the cell administrator: % dce_login> cell_name%Enter Principal Name: cell_admin cell_name% Enter Password <cell_admin password> Obtain DCE prompt and invoke registry edit functions: cell_name% rgy_edit	current site is registry server at /.../<cell_name>/subsys/dce/sec/master rgy_edit prompt is displayed: rgy_edit>		
2	Initiate the display of standard policies: rgy_edit=> po	The registry contents of the standard policies is displayed. The standard policies include account lifespan, minimum password length, password expiration, and characters allowed in the password. Changes may be made if desired.		
3	Initiate the display of authentication policies: rgy_edit=>au	The registry contents of the authentication policies is displayed. The authentication policies include maximum ticket renewable time, and maximum ticket lifetime. Changes may be made if desired.		
4	Initiate the display of properties: rgy_edit=> prop	A complete listing of all the current properties is displayed. The properties include master registry read-only condition, hidden password property, low UNIX ID, maximum UNIX ID, minimum ticket lifetime in minutes, and default ticket lifetime in hours.	As described in Test Objective #233, it is important to configure the Authentication Server with proper settings that implement site security policies. It is also important to note that these security parameters can be so constraining that productivity is hampered and system performance is affected. A proper balance of security	

			and functionality must be reached; it then can be implemented using DCE.	

Topic: Distributed Computing

Subtopic: DCE Account Creation Defaults

Test Objective 245 Verify that DCE account creation defaults are properly configured.

DII COE SRS Requirement: None Identified

Rationale:

#	Required Action	Expected Results	Comments	Ö
1	Refer to Test Actions in Objectives #233, 234, and 244.			

Topic: Distributed Computing

Subtopic: DCE Names

Test Objective 237 Verify that the DCE cell has a cell name.

DII COE SRS Requirement: None Identified

Rationale: An appropriate DCE cell name is important because: 1) DCE cells that will participate in the global namespace must have unique names to differentiate them from cells in other organizations, and 2) a uniquely identified cell name is critical to the operation of DCE security. The cell name is the basis for authentication within that cell.

#	Required Action	Expected Results	Comments	Ö
1	To determine the DCE cell name, review of a DCE configuration file is required. Login to DCE as "cell_admin": % dce_login> cell_admin % password <cell_admin password> Obtain DCE prompt. The DCE prompt contains the DCE cell name. To further verify cell name information: Change directory to where DCE configuration information is located: % cd /opt/dcelocal Lists the contents of file: % cat dce_cf.db	The contents of the dce_cf.db file should contain two names: one name is the DCE cell name and the second is the host name. Visually verify that names are correct.	DCE can support either the Domain Naming Service (DNS) or the Global Directory Service (GDS) naming conventions for communication outside of the DCE cell. However, these are NOT SUPPORTED SIMULTANEOUSLY; one or the other must be chosen. ice454.8 -2	

			space. For example, a DCE DNS principal name may appear as follows: "John_Doe@hostname.Army.mil"	

Topic: Distributed Computing

Subtopic: DCE Names

Test Objective 238 Verify that global names exist for all objects, applications, machines, and users.

DII COE SRS Requirement: None Identified

Rationale: In order for various object to be used for discretionary access control checks, each must be identified and authenticated prior to access control checking. This is accomplished in a DCE cell by the use of global names. Global names can be used outside the DCE cell in which the object is registered. This global name is used to perform appropriate access checks when attempting to access an object in a different cell.

{This checklist item must be verified when a complete set of principals, users, machines, and objects are installed.}

#	Required Action	Expected Results	Comments	Ö
1	TBD			

Topic:	Distributed Computing
Subtopic:	DCE Server
Test Objective 241	Verify that each DCE Core server has an Access Control List (ACL) manager.
DII COE SRS Requirement:	None Identified
Rationale:	Resources such as severs, directories, and files can have an associated access control list (ACL) that specifies which operations can be performed by which user. A program called an ACL manager is necessary to maintain these ACLs and enforce the access control policy on each server.

#	Required Action	Expected Results	Comments	ü
1	Log in to DCE as the cell administrator: %dce_login %Enter Principal Name: cell_admin %Enter Password: <cell_admin password> Obtain DCE prompt and invoke DCE control program: cell_name% cell_name%dcecp	DCE control program prompt is displayed: dcecp>		
2	View and verify contents of Security Server ACL: dcecp>acl show /.../<cell_name>/subsys/sec View and verify contents of CDS clearinghouse ACL: dcecp>acl show /.../<cell_name>/<machine_name>_ch View and verify contents of DTS server ACL: dcecp>acl show /.../<cell_name>/hosts/<machine_nema>/dts-entity		In the filespace, ACLs are an extension of the UNIX system file-protection model. While UNIX file system permissions are limited to the protection of files and directories, DCE ACLs can also control access to nonfile system objects, such as entries in a database and objects registered in the cell namespace. Every ACL is managed by an ACL manager. An ACL manager determines a principal's authorization to perform an operation on an object by reading the object's ACL to find the appropriate entry (or entries) that matches some privilege attribute possessed by the principal. If the type of access requested by the principal is one of the permissions listed in the matching entry, then the ACL manager allows the principal to perform the requested operation. If the requested permission is not listed	

			in the matching ACL entry, or is denied by a mask, permission to perform the operation is denied. Permission is also denied if the ACL contains no matching privilege attribute entry. DCE components and applications can use different kinds of ACLs to protect their respective resources. The types of ACLs and their exact effects depend on how they are defined by the ACL manager for the specific component or application. ACLs and ACL managers are optional on many servers. However, they should exist for file servers, security servers, time servers, and directory servers. When the register database is created, the Principal, Group, and Organization directories and the Policy object are given initial ACLs. As new objects are created in the registry, they inherit their ACLs from the appropriate directory ACL. The initial ACLs, created when the registry database is created, contain permissions for the user, user_obj, other_obj, and unauthorized users for principals and group objects. Likewise, it contains permissions for user, other_obj, and unauthorized users for policy and organization objects. Finally, it contains permissions for the user, othr_obj, and unauthenticated users for directory objects. ACLs are optional for servers within DCE. However, DCE release 1.1 has ACL Manager Library enhancements to ease the development of servers by providing server writers with an ACL manager for use with all servers.	

Topic: Distributed Computing

Subtopic: DCE Server

Test Objective 242 Verify that DCE Core Component Server has an ACL associated with it.

DII COE SRS Requirement: None Identified

Rationale: ACLs indicate who can use the object and what operations can be performed on that object.

#	Required Action	Expected Results	Comments	Ö
1	Refer to DCE Security Test Objective #241 for a complete description of this test.	Objects on the core DCE servers indeed have ACLs and these ACLs limit access to the appropriate principals.	DCE components and applications can use different kinds of ACLs to protect their respective resources. The types of ACLs and their exact effects depend on how they are defined by the ACL manager for the specific component or application. ACLs and ACL managers are optional on many servers. However, they should exist for file servers, security servers, time servers, and directory servers.	

Topic: Distributed Computing

Subtopic: DNS/GDS Global Names

Test Objective 239 Verify that DNS or GDS Global names exist.

DII COE SRS Requirement: None Identified

Rationale: If DNS is planned to be used as the global name service, the DCE cell name needs to conform to the ARPA Internet Domain System convention for site names. The name must have two levels (e.g., abc.com, dod.mil, etc.) that are registered with the Network Information Center (NIC).

For NIC name registration, contact:

Government Systems Inc.
Attention: Network Information Center (NIC)
4200 Park Meadow Drive
Chantilly, VA 22021
800-365-3642 or 703-802-4535
hostmaster@nic.ddn.mil

Alternatively, if GDS is planned to be used as the global name service, the DCE cell name needs to conform to the ANSI delegated X.500 names subordinate to the C=US entry. The name must contain an official organization name, and optionally multiple sub-organization names.

For X.500 name registration, contact:

American National Standards Institute
1430 Broadway
New York, NY 10018
212-642-4976

#	**Required Action**	**Expected Results**	**Comments**	Ö
1	This is a procedural test. Check network documentation to insure that proper procedures were followed to determine and assign an appropriate cell name in one of the two systems supported by DCE. An official cell name must exist and be registered with the proper administrative office.	A global name exists and is properly registered with the appropriate office.		

Topic: Distributed Computing

Subtopic: Kerberos Authentication/Security Services

Test Objective 228 Verify that Kerberos network authentication/security services are configured correctly.

DII COE SRS Requirement: None Identified

Rationale: Kerberos is a significant component providing many security features for DCE. It is the Kerberos features that Identify and Authenticate (I&A) individuals to the system and then pass this I&A information to other servers in a secure manner. This I&A information is used by servers as the basis for access control decisions made by each server. It is imperative that the Kerberos security features are operating properly.

#	Required Action	Expected Results	Comments	Ö
1	Log in to DCE as the cell administrator: %dce_login %Enter Principal Name: cell_admin %Enter Password: <cell_admin password> Obtain DCE prompt and invoke registry edit functions: cell_name% cell_name%rgy_edit	current site is registry server at /.../<cell_name>/subsys/dce/sec/master rgy_edit prompt is displayed: rgy_edit>		
2	Initiate the display of standard policies. rgy_edit=> po	The registry contents of the standard policies is displayed. The standard policies include account lifespan, minimum password length, password expiration, and characters allowed in the password. Changes may be made if desired.		
3	Initiate the display of authentication policies. rgy_edit=>au	The registry contents of the authentication policies is displayed. The authentication policies include maximum ticket renewable time, and maximum ticket lifetime. Changes may be made if desired.		
4	Initiate the display of properties. rgy_edit=> prop	A complete listing of all the current properties is displayed. The properties include master registry read-only condition, hidden password property, low UNIX ID, maximum UNIX ID, minimum ticket lifetime in minutes, and default ticket lifetime in hours.	Kerberos currently provides the authentication security services for DCE through the GSSAPI. The underlying Kerberos (and other) security features are invoked through that interface. It is important to note, however, that Kerberos "could" be replaced by another security service that	

			conforms to the GSSAPI without application software impact. There are plans (possibly in future DCE releases) to provide a public/private key mechanism as an alternative to Kerberos. Authentication services are provided primarily by Kerberos. Principal names and passwords provide authenticity; encrypted "tickets" are created and used to pass authentication information to servers; and the privilege attributes for principals are also provided by the authentication server. As described in Objective #233, it is important to configure the Authentication Server with proper settings that implement site security policies. It is also important to note that these security parameters can be so constraining that productivity is hampered and system performance is affected. A proper balance of security and functionality must be reached; it then can be implemented using DCE.	

Topic: Distributed Computing

Subtopic: Master Registry

Test Objective 243 Verify that the cell has only one master registry.

DII COE SRS Requirement: None Identified

Rationale: It is highly unusual to have more than one registry master running on the network. It is appropriate to have one master and a number of replicated slaves for the purpose of load balancing, performance improvement, and backup in the event that the master is unavailable. However, only the master registry is updated by the security or cell administrators, and the master handles keeping data in the slave units up to date.

#	Required Action	Expected Results	Comments	Ö
1	Log in to DCE as the cell administrator: %dce_login %Enter Principal Name: cell_admin %Enter Password: <cell_admin password> Obtain DCE prompt and invoke sec_admin functions: cell_name% cell_name%sec-admin	Cell information is displayed: Default Replica: /.../<cell_name>/subsys/dce/sec/master Default cell: /.../<cell_name> Prompt is displayed: sec_admin>		
2	Issue the "lrep" command with the state option to display all registry servers and their status: sec_admin: lrep -state	The master and slave security servers and their status is listed as follows: (master) "server name" "state: status" "date and time" (slaves) "server name" "state: status" "date and time" "server name" "state: status" "date and time" "server name" "state: status" "date and time" "server name" "state: status" "date and time" Verify that only one master registry is in operation and that slaves are also running if configured by the security administrator. In the event that there is more than one master registry identified and operational, the following procedure		

		will turn a master into a slave server.		
3	Set the chosen master to the default host: sec_admin: set -h <name of host machine to become a slave> Set the default host to become a slave: sec_admin: become -slave Verify the change: sec_admin: lrep -state	The selected master has been reassigned as a slave unit. This change has been verified.		

Topic: Distributed Computing

Subtopic: Master Server

Test Objective 236 Verify that the master server is available and physically secure.

DII COE SRS Requirement: None Identified

Rationale: The DCE Security Service provides safeguards for network security protecting information that is transmitted across the network by guaranteeing the identity of all principals. Since the security server and the database it serves reside on a local machine, the registry database is only as secure as the security provided by the machine on which it resides. In addition to ensuring that sensitive data can be accessed on the local machine only by "root," physical security for the machine on which the security server resided must also be provided.

#	Required Action	Expected Results	Comments	Ö
1	Visually inspect the location where the DCE Security Server(s) is(are) operating. Insure that physical security measures are maintained and that only authorized personnel are allowed to access the security server.	The Security Server is in a protected environment.	It may also be appropriate to encourage the use of a log that will manually track access to the DCE Security Servers.	

Topic: Distributed Computing

Subtopic: Registry Database

Test Objective 230 Verify that all principals are registered in the DCE Registry database.

DII COE SRS Requirement: None Identified

Rationale: Principals are users of the system. Principals can be interactive principals (human users) or non-interactive principals (servers, machines, and cells). In order for principals to be authenticated to the various system servers, they must be registered in the Registry database.

#	Required Action	Expected Results	Comments	ü
1	Log in to DCE as the cell administrator %dce_login %Enter Principal Name: cell_admin %Enter Password: <cell_admin password> Obtain DCE prompt and invoke registry edit functions: cell_name% cell_name%rgy_edit	current site is registry server at /.../<cell_name>/subsys/dce/sec/master rgy_edit prompt is displayed rgy_edit>		
2	Set the registry domain to principals: rgy_edit> do principal View all principals in the registry database: rgy_edit> view	The entire contents of the registry database of principals is displayed.		
3	View the complete set of information for the principal name specified. rgy_edit> view [principal] -f Repeat this command to view and verify information for a number of principals.	A specific principal's information is displayed. This information includes the principal's primary and full name, UNIX ID and UUID, the principals' object creation quota, and an indication of whether or not the primary name is an alias.	For principals to engage in authenticated transactions, they must be registered in the registry database. Authentication information is provided for servers in order for the servers to make access control decision upon the objects under the server's control. If a principal is not registered, authentication information is not provided by DCE's security services and therefore, cannot be used as a basis for making access control decisions. This results in unauthenticated access to objects by that user. In many instances, this results in a much more	

			constrained access control decision. If a full listing of a particular principal is required enter "view [principal} -f" at the rgy_edit prompt. This will result in a complete listing of information in the registry database for the named principal.	

Topic: Distributed Computing

Subtopic: Registry Database

Test Objective 231 Verify that all groups are registered in the DCE Registry database.

DII COE SRS Requirement: None Identified

Rationale: Groups are used to provide system servers with authentication information for groups of principals. Group members (all principals) will share the same access control information. Discretionary access control decisions are based upon "owner, group, and other" -enforced permissions. Therefore, all members of a specific group could all have similar access by being members of the same group.

#	Required Action	Expected Results	Comments	Ö
1	Log in to DCE as the cell administrator: %dce_login %Enter Principal Name: cell_admin %Enter Password: <cell_admin password> Obtain DCE prompt and invoke registry edit functions: cell_name% cell_name%rgy_edit	current site is registry server at /.../<cell_name>/subsys/dce/sec/master rgy_edit prompt is displayed: rgy_edit>		
2	Set the registry domain to groups: rgy_edit> do group View all groups in the registry database: rgy_edit> view	The entire contents of the registry database of groups is displayed.		
3	View the complete set of information for the group name specified: rgy_edit> view [groupname] -f Repeat this command to view and verify information for a number of groups.	The complete set of group information is displayed. This information includes the group's primary and full name, UNIX ID and UUID, an indication of whether or not the primary name is an alias, and other group specific information.		
4	View the group membership set: rgy_edit> view [groupname] -m Repeat this command to view and verify membership lists for many or all groups.	A complete listing of all the group's members are displayed.		

Topic: Distributed Computing

Subtopic: Registry Database

Test Objective 232 Verify that all organizations are registered in the DCE Registry database.

DII COE SRS Requirement: None Identified

Rationale: Organizations should be registered in the database to limit access that otherwise may not be granted.

#	**Required Action**	**Expected Results**	**Comments**	Ö
1	Log in to DCE as the cell administrator: %dce_login %Enter Principal Name: cell_admin %Enter Password: <cell_admin password> Obtain DCE prompt and invoke registry edit functions: cell_name% cell_name%rgy_edit	current site is registry server at /.../<cell_name>/subsys/dce/sec/master rgy_edit prompt is displayed: rgy_edit>		
2	Set the registry domain to organizations: rgy_edit> do org View all organizations in the registry database: rgy_edit> view rgy_edit=> view	The entire contents of the registry database of organizations is displayed.		
3	View the complete set of information for the organization name specified: rgy_edit> view [orgname] -f Repeat this command to view and verify information for all organizations.	The complete set of organization information is displayed. This information includes the organization's primary and full name, UNIX ID and UUID, an indication of whether or not the primary name is an alias, and other organization specific information.		
4	View the organization membership set: rgy_edit> view [orgname] -m	A complete listing of all the organization's members are displayed.		
5	View the organization's policy information: rgy_edit> view [orgname] -po Repeat this command to view and verify information for all	A complete listing of all the organization's policy information is displayed. This information includes account lifetime, minimum password length, password lifetime, and various	If the default security parameters are left unchanged after cell initialization, anyone logged into a DCE client machine connected to the network can search through the entire cell. If, in addition to read	

	organizations within the DCE cell.	other organization specific information.	permissions, write permissions were granted on behalf of unauthenticated users, everyone in the network could create and edit directories, names, entries, and files. Obviously, this is not a secure arrangement. It is, therefore, important to display and review all information regarding principals, group membership, and organizations to guarantee that current settings conform to the site security policies. As users leave or are reassigned, they should be removed from group memberships that are no longer required. The precise access control that can be achieved with DCE authentication and authorization is very complete. If the site requires high security, it can be achieved using all the security features of DCE. It can be configured that only authenticated users defined in the cell's registry, have access to any cell resource. Users can be denied access from foreign cells regardless of whether they can be authenticated. Furthermore, if a high degree of access control granularity is necessary, the use of authorization groups can be abandoned and it be required that each user be granted permission to individual cell resources based solely on permissions granted to that specific user. The interval at which a user's authentication credentials expire can be adjusted. The default ticket expiration can be changed from the default of ten (10) hours to minutes if it is necessary. The tradeoff to be considered as cell security is tightened, is that of administration. The administrative burden in a cell with a large number of principals, groups, and changes may be significant.	

Topic: Distributed Computing

Subtopic: Registry Database

Test Objective 233 Verify that administrative policies and procedures are described in the DCE Registry database.

DII COE SRS Requirement: None Identified

Rationale: These administrative policies and procedures represent the configuration as new users are added to the database. These parameters clearly define the "tightness" of DCE security to be implemented at the site. It is important that these parameters accurately reflect the security intent of the site.

#	Required Action	Expected Results	Comments	Ö
1	Log in to DCE as the cell administrator: %dce_login %Enter Principal Name: cell_admin %Enter Password: <cell_admin password> Obtain DCE prompt and invoke registry edit functions: cell_name% cell_name%rgy_edit	current site is registry server at /.../<cell_name>/subsys/dce/sec/master rgy_edit prompt is displayed: rgy_edit>		
2	Initiate the display of standard policies: rgy_edit> po	The registry contents of the standard policies is displayed. The standard policies include account lifespan, minimum password length, password expiration, and characters allowed in the password. Changes may be made if desired.		
3	Initiate the display of authentication policies: rgy_edit=>au	The registry contents of the authentication policies is displayed. The authentication policies include maximum ticket renewable time, and maximum ticket lifetime. Changes may be made if desired.		
4	Initiate the display of properties: rgy_edit=> prop	A complete listing of all the current properties is displayed. The properties include master registry read-only condition, hidden password property, low UNIX ID, maximum UNIX ID, minimum ticket lifetime in minutes, and default ticket lifetime in hours.	These policies and properties, in conjunction with the principal, group, and organization entries, establish the security settings for the cell. For stricter security, set the password expiration to be as short as possible; set the password lifetime to be short; account lifespan to be short; password length to be eight characters or more; and for the	

			password to contain non-alphanumeric characters. All of the registry database attributes must be examined to provide the proper level of security with an appropriate amount of cell security administration. It would be wise for a site to study and establish a policy prior to the installation and configuration of the DCE cell.	

Topic: Distributed Computing

Subtopic: Registry Database

Test Objective 234 Verify that all user accounts are registered in the DCE Registry database.

DII COE SRS Requirement: None Identified

Rationale:

#	Required Action	Expected Results	Comments	Ö
1	Login to DCE as "cell_admin" % dce_login> cell_admin % password <enter cell_admin pw> Obtain DCE prompt and invoke registry edit functions: % <dceshared directory name>rgy_edit	current site is registry server at /.../<cell_name>/subsys/dce/sec/master rgy_edit prompt is displayed: rgy_edit>		

2	Set the registry domain to accounts:
	rgy_edit=> do account
	
	View all accounts in the registry database:
	rgy_edit=> view
		The entire contents of the registry database of accounts is displayed.		

3	View the complete set of information for the account name specified: rgy_edit=> view [account] -f Repeat this command to view and verify information for many or all installed accounts within this DCE cell.	A specific account's information is displayed. This information includes the account's password status, expiration date, roles the account MAY assume (e.g., client principal, server principal), certificate information, and other account information and statistics.		

Topic:	Distributed Computing
Subtopic:	Replicated Database
Test Objective 235	Identify and insure that all slave and/or replicated databases are operational.
DII COE SRS Requirement:	None Identified
Rationale:	All DCE servers provide some information that is necessary for proper cell operations. These include the Security Server, the Cell Directory Server, the Global Directory Server, the Registry Server, etc.

#	Required Action	Expected Results	Comments	Ö
1	Login to DCE as "cell_admin": % dce_login> cell_admin % password <cell_admin password> Obtain DCE prompt and invoke command to show all cell servers: cell_name% cell_name%dcecp -c cell show	A list of servers is displayed. All master and slave servers and their status are listed as follows: secservers (master) "server name" "state: status" "date and time" (slaves) "server name" "state: status" "date and time" "server name" "state: status" "date and time" cdsservers (master) "server name" "state: status" "date and time" (slaves) "server name" "state: status" "date and time" "server name" "state: status" "date and time" dtsservers (master) "server name" "state: status" "date and time" (slaves) "server name" "state: status" "date and time" "server name" "state: status" "date and time" hosts A list of hosts within the DCE cell is also displayed here.	For the cell to operate properly, the following servers must be installed and configured as a minimum; they are: a CDS server, a DTS server, and a Security Server. It is possible that all servers are configured on the same machine. There are practical advantages to this configuration; they are: ease of installation and configuration, ease of administration, increased performance and reliability, economy, and convenience. Additionally, there are disadvantages for configuring the servers on one machine; they are: avoiding a single point of failure, avoiding possible performance bottlenecks, accommodating special security requirements, and matching the machine to the service. It is important that each cell have the required servers. It is less important as to where the servers are located and installed. Server configuration may be a site specific operation and no two sites may have the same philosophy, number of clients and servers, and	

			available machines to perform server functions.	

Topic: Distributed Computing

Subtopic: Security Namespace

Test Objective 240 Verify that security namespaces exist for groups, group directories, principals, and principal directories.

DII COE SRS Requirement: None Identified

Rationale: In order to protect various directories and files using DCE permissions for owners, groups, authenticated users, and unauthenticated users, it is important to have protected space for many objects. This protected space is used as the home directory of each user and group and is the basis for all discretionary access control decisions.

{This checklist item must be verified when a complete set of users, and groups is installed.}

#	Required Action	Expected Results	Comments	Ö
1	TBD			

Topic: Distributed Computing

Subtopic: Servers

Test Objective 229 Verify that critical servers are operating correctly.

DII COE SRS Requirement: None Identified

Rationale: All DCE servers provide some information that is necessary for proper cell operations. These include the Security Server, the Cell Directory Server, the Global Directory Server, the Registry Server, etc. This test verifies security server operation.

#	Required Action	Expected Results	Comments	Ö
1	Log in to DCE as the cell administrator: %dce_login %Enter Principal Name: cell_admin %Enter Password: <cell_admin password> Obtain DCE prompt and invoke sec_admin functions: cell_name% cell_name% sec_admin	Default Replica: /.../<cell_name>/subsys/dce/sec/master Cell information is displayed: Default cell: /.../<cell_name> Prompt is displayed: sec_admin>		
2	Issue the "lrep" command with the state option to display all registry servers and their status: sec_admin> lrep -state	All master and slave servers and their status are listed as follows: (master) "server name" "state: status" "date and time" (slaves) "server name" "state: status" "date and time" "server name" "state: status" "date and time" "server name" "state: status" "date and time" "server name" "state: status" "date and time"	For the cell to operate properly, the following servers must be installed and configured as a minimum; they are: a CDS server, a DTS server, and a Security Server. It is possible that all servers are configured on the same machine. There are practical advantages to this configuration; they are: ease of installation and configuration, ease of administration, increased performance and reliability, economy, and convenience. Additionally, there are disadvantages for configuring the servers on one machine; they are: avoiding a single point of failure, avoiding possible performance bottlenecks, accommodating special security requirements, and matching the machine to the service. It is important that each cell have	

			the required servers. It is less important as to where the servers are located and installed. Server configuration may be a site specific operation and no two sites may have the same philosophy, number of clients and servers, and available machines to perform server functions.	

Topic: Distributed Computing

Subtopic: Version

Test Objective 227 Verify the DCE version.

DII COE SRS Requirement: None Identified

Rationale: Various security features were released on an interim basis from DCE Release 1.0.1 to Release 1.1. It is important that all security features be available and all previous release defects be corrected. Additionally, security server replication and master/slave operations were enhanced in DCE Release 1.1.

#	Required Action	Expected Results	Comments	Ö
1	Log on to UNIX system as root Log in to DCE as the cell administrator: %dce_login %Enter Principal Name: cell_admin %Enter Password: <cell_admin password> Obtain DCE prompt and run executable to display DCE release information: cell_name% cell_name% dce_version Obtain DCE prompt and run executable to display DCE release information: cell_name% cell_name% dce_version	DCE Version is Release 1.1 or later	DCE releases have been continually enhanced to provide additional security as well as functional features. DCE Release 1.1 provides an interface to the underlying security mechanism by means of the Generic Security Services - Application Programming Interface (GSSAPI). Additionally, many of the security servers are able to be replicated and assume master operation in the event that the initial master becomes inoperative. The OSF DCE has been certified to execute properly on the following platforms by the OSF. OSF provides support for these platforms. This list is not inclusive, new platforms are added on a regular basis: HP700 executing the HP-UX operating system, RS6000 executing the AIX 3.2.4 operating system, PC486 executing the OSF/1 1.2 as an operating system, and MX300 executing the SINIX (SVR4-based) operating system.	